



**WELCOMING COMMENTS BY
NATIONAL COUNTERINTELLIGENCE EXECUTIVE DR. JOEL F. BRENNER
DNI -PRIVATE SECTOR WORKSHOP ON EMERGING TECHNOLOGIES**

Carnegie Endowment for International Peace, Washington, DC
7 December 2006

Boundaries of every kind are eroding—legally, behaviorally, electronically—in all aspects of our lives:

- Between the public and private behavior of ordinary people; for example, the sense of dress and decorum appropriate to the home, the street, the office, or houses of worship.
- Between the public and private—that is, secret—behavior of governments.
- Between the financing, legal norms, and research activities of public as opposed to private institutions; universities, for instance.
- Between state and non-state actors and the relative size of the resources they control.

Cyber boundaries are also eroding—and not always in ways we like—but simply because we are sometimes helpless to enforce them. Theoretical physicists could no doubt add still more profound examples.

Trends like this don't appear in isolation. They show up across the board, because cultures are all of a piece.

Similarly, the equivalence in the minds of many people between national security and government secrets is also eroding—has eroded, in fact—almost completely. That is, when it comes to national security, the boundary between the public and the private has more or less vanished. The infrastructure we need to protect, the technology and know-how we need to protect are in no way restricted to government property. Terrorists in hijacked jetliners plow indiscriminately into the headquarters of government departments and private office buildings. The technology our military relies on is developed in most cases in the private sector or in academia. Electric grids, information systems, financial networks, air-traffic control systems are all targets now.

The national security of a nation depends on its military, of course, and on its will to protect itself. But in a larger sense it also depends on its wealth and its influence, both of which are heavily technology reliant.

At the same time, the world is speeding up—accelerating. We experience this in the pace of our daily lives, in product cycles and fashion cycles, in the dissemination of information, in the capacity of our electronic systems, in the speed at which products are copied and pirated—in just about every way one can think of. So much so that business people increasingly realize that their ability to profit from their own innovation depends on their ability to get that product or technology to market faster than ever—before it becomes obsolete, out of fashion, or ripped off by a low-overhead pirate with no R&D costs.

The same thing is true in the intelligence business. When General Hayden was the Director of NSA, he used to say that all advantage in signals intelligence—the electronic stuff—was transient. Now that he's done a tour as Principal Deputy Director of National Intelligence and has moved on to head the CIA, he just says that *all* intelligence advantage is transitory. And of course he's right.

Those of us in *counterintelligence* are in the business of protecting America's secrets. Our responsibilities require us not only to understand and thwart the systematic efforts of foreign intelligence services to insert spies into the workings of our government, but also to thwart the increasingly systematic penetrations of public and private electronic networks, which are the backbone of our communications, the storehouse of our technology, and the nervous system of our economy and system of government.

These systems, I'm afraid to say, are in many cases terribly porous and insecure—vulnerable not only to casual hackers but even more so to professional electronic thieves and powerful, state-sponsored electronic attacks. But we Americans want convenience—we want seamless interconnectivity—yet we know from experience that whenever convenience butts heads with security, convenience wins. And so our vulnerabilities multiply.

The fact is, intellectual thieves are eating our lunch—eating *your* lunch. The public and private sectors are both leaking badly. I'm not talking about just the pirating of DVDs and movies in Asia. I'm talking about significant technologies that are walking out of our laboratories on electronic disks, walking onto airplanes bound for foreign ports, and re-entering the country as finished products developed by foreign entrepreneurs. In effect, we're buying back our own technology. This is bad enough when we're talking about commercial innovation. But when we're talking about technology with substantial defense applications, we're talking about losses of intellectual capital that in wartime could cost many lives or our fellow citizens. These losses are occurring, and they are occurring in a targeted, systematic manner.

Protecting innovative technology before it can be patented or classified is an urgent task, and it is difficult. If any of us knew how to do it, he'd be very rich, because it's a question of handicapping basic research.

Which brings me to why we're here today. This is Pearl Harbor Day—the anniversary of the Nation's quintessential counterintelligence failure. And it was a failure not merely of communication within the government, but also of a failure of scientific imagination—the Navy was certain that the waters of the harbor were too shallow for torpedoes. They couldn't conceive that scientists in another country—an Asian country no less—could have solved this very problem, which they had done.

So we in the counterintelligence business are straining to peer over the horizon, to identify technologies that will disrupt the way we think and work and do business. And so, for a variety of reasons, are all of you. Each of you and the institutions you represent are jewels in the clockwork of American enterprise, intellect, and wealth. You succeed or fail depending on whether you anticipate the future better than the next guy.

And so I welcome you to this public-private conference whose purpose is the invariability fallible but vital effort to think imaginatively about what lies around the corner, over the horizon, beyond tomorrow. And to think and talk together about the emerging technologies that will continue to erode our boundaries, accelerate change, and confound our ability to control them.

The task we set for ourselves today is difficult, daunting, and exciting. Enjoy yourselves. Get to know one another. Think big thoughts. Our country needs us to be good at this—needs us to enrich the public sector with private know-how and to imbue the private sector with a renewed sense of public purpose.

Thank you.